

信息安全漏洞周报

2010年8月30日-2010年9月5日

2010年第34期

本周漏洞基本情况

本周信息安全漏洞威胁整体评价级别为中。

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 108 个，其中高危漏洞 16 个、中危漏洞 51 个、低危漏洞 41 个。上述漏洞中，可利用来实施远程攻击的漏洞有 58 个。经跟踪发现，网上已经出现针对 windows 平台下多个应用软件“dll 劫持漏洞”的零日攻击代码，请相关用户注意做好相关防护措施。本周收录的安全漏洞中，已有 30 个漏洞由相关厂商提供了修补方案，建议用户及时下载补丁更新程序，避免遭受网络攻击。

本周重要漏洞信息

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、Microsoft 多款产品存在 DLL 劫持漏洞

受Windows平台的“dll 劫持漏洞”影响，Microsoft 的Vista、Office Groove2007、Address Book、Visio 2003、Windows 7、Windows Movie Maker、PowerPoint 2010等产品被披露可进行DLL劫持，攻击者可利用这些漏洞进行拒绝服务攻击或以应用程序权限执行特定代码。具体漏洞包括：Microsoft Group Converter DLL 劫持漏洞、Microsoft Internet Connection Signup Wizard DLL劫持漏洞、Microsoft Office Groove 2007 DLL劫持漏洞、Microsoft Address Book DLL劫持漏洞、Microsoft Visio 2003 DLL劫持漏洞、Microsoft Windows 7 wab.exe DLL劫持漏洞、Microsoft Windows Movie Maker <= 2.6.4038.0 DLL劫持漏洞、Microsoft PowerPoint 2010 DLL劫持漏洞。目前Microsoft尚未发布正式的补丁程序修复上述安全漏洞，建议相关用户应提高警惕并做好安全防范工作，具体防范措施如下：1) 不访问不可信的远程文件系统，不打开不可信的文件；2) 在防火墙或系统中禁用文件共享协议（SMB）；3) 采用微软安全建议中提供的软件工具；4) 关注厂商主页，及时获取修补方案。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01866>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01868>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01870>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01885>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01837>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01841>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01843>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01881>

2、Adobe 多款产品存在安全漏洞

受 Windows 平台的“dll 劫持漏洞”影响，Adobe Photoshop CS2、Dreamweaver CS5、Adobe Acrobat Reader、Adobe Premier Pro CS4 等产品本周被披露可进行 DLL 劫持。此外，Adobe 公司相关产品还存在其他漏洞。攻击者可利用这些漏洞以应用程序权限执行特定代码。具体漏洞包括：Adobe Device Central CS5 DLL 劫持漏洞、Adobe Premier Pro CS4 不安全加载漏洞、Adobe Captivat 不安全库文件加载漏洞、Adobe Extension Manager CS5 v5.0.298 存在 dwmapi.dll 漏洞、Adobe Photoshop CS2 DLL 劫持漏洞、Adobe Dreamweaver CS5 DLL 劫持漏洞、Adobe ExtendedScript Toolkit CS5 v3.5.0.52 存在 dwmapi.dll 漏洞、Adobe Acrobat Reader 内存损坏漏洞。目前 Adobe 尚未发布补丁或更新程序修复上述漏洞，建议相关用户继续关注厂商主页以及及时获取修补方案。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01878>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01876>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01817>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01790>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01865>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01882>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01855>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01849>

3、Wireshark存在多个安全漏洞

Wireshark是一款开放源代码的网络协议分析工具。Wireshark存在多个安全漏洞，远程攻击者可利用漏洞使应用程序崩溃。具体漏洞信包括：Wireshark <= 1.2.10 DLL 劫持漏洞、Wireshark的IPMI解析器、ASN.1 BER解析器和GSM ARR解析器存在漏洞、Wireshark的SigComp通用解压缩虚拟机存在覆盖缓冲区漏洞。目前Wireshark Wireshark 1.2.10和1.0.15已修复上述安全漏洞，建议相关用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01824>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01823>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01822>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01821>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01838>

4、IBM DB2 存在安全漏洞

IBM DB2是一款大型的关系型数据库管理系统，面向电子商务、商业资讯、内容管理、客户关系管理等应用，可运行于AIX、HP-UX、Linux、Solaris、Windows等系统。IBM DB2

存在多个安全漏洞，远程攻击者可以利用这些漏洞获取敏感信息或实施拒绝服务攻击。具体漏洞包括：IBM DB2 SYSIBMADM schema、DB2DART和FP2存在权限许可和访问控制漏洞、IBM DB2存在未明拒绝服务漏洞、IBM DB2 在列举特殊组和用户时存在安全漏洞、IBM DB2 DB2STST存在安全漏洞。目前IBM 9.1 Fix Pack 9、9.5 Fix Pack 6和9.7 Fix Pack 2已修复上述安全漏洞，建议相关用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01782>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01781>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01780>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01853>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01850>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01847>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01846>

小结：上述漏洞信息中，除 Microsoft 和 Adobe 多款产品存在的安全漏洞尚未发布补丁或更新程序外，其它漏洞信息已有相应的安全补丁或更新程序。这些漏洞对用户的信息安全和公共互联网网络安全构成威胁，请使用上述软件的相关机构和个人及时采取安全防范措施。

本周重要漏洞修补信息

本周，CNVD 整理和发布以下重要安全修补信息。

1、Cisco 发布安全公告

9月2日，Cisco 发布安全公告 cisco-sa-20100827-bgp，修复 Cisco IOS XR 3.4.0 至 3.9.1 版本在启用 BGP 时不能正确处理未识别的传递属性的漏洞。CNVD 提醒广大用户为避免遭受漏洞影响请及时下载补丁更新。

补丁下载链接：<http://www.cnvd.org.cn/patch/914>

本周要闻速递

1、思科 IOS 现严重漏洞，致 1% 互联网瘫痪

9月3日，RIPE NCC(Reseaux IP Europeens Network Coordination Centre)和杜克大学的一些研究者发现运行思科 IOS XR 操作系统的路由器存在一个 bug。他们通过 RIPE NCC 系统分发实验性的 BGP (Border Gateway Protocol)数据，在几分钟以内，许多互联网上的路由器便无法访问。据分析，由于这些实验性的数据比传统的 BGP 路由信息要大一些，运行思科 IOS XR 操作系统的路由器在获取这些实验性的数据后便将其损坏，并将这些已经损坏的信息发送到其他路由器上。许多收到已损坏信息的路由器只是简单地中断和思科路由器（此

处的路由器指发送损坏信息的路由器)的连接,从而导致部分互联网出现无法访问的情况。漏洞曝出后,思科已及时发布安全公告修复此安全漏洞。

参考链接: <http://sec.chinabyte.com/449/11520449.shtml>

2、微软发布临时工具解决 DLL 劫持漏洞

北京时间 9 月 1 日消息,据国外媒体报道,微软已经发布了一款临时工具以解决 DLL 劫持漏洞问题。这款临时工具可拦截攻击者利用 DLL 加载漏洞在管理员升级受感染应用软件时发起的攻击。微软已经证实,管理员需要用一定的时间来检查和升级所有受感染的微软和第三方应用软件。微软保证在发布了针对该漏洞的安全建议书之后,会解决其软件中的 DLL 劫持漏洞。

参考链接: <http://www.cert.org.cn/articles/news/common/2010090325119.shtml>

关于 CNVD

国家信息安全漏洞共享平台(China National Vulnerability Database, 简称 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库,致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

关于 CNCERT

国家互联网应急中心的全称是国家计算机网络应急技术处理协调中心(英文简称是 CNCERT 或 CNCERT/CC)成立于 1999 年 9 月,是工业和信息化部领导下的国家级网络安全应急机构,致力于建设国家级的网络安全监测中心、预警中心和应急中心,以支撑政府主管部门履行网络安全相关的社会管理和公共服务职能,支持基础信息网络的安全防护和安全运行,支援重要信息系统的网络安全监测、预警和处置;国家互联网应急中心在我国大陆 31 个省、自治区、直辖市设有分中心。

网址: www.cert.org.cn

邮箱: vreport@cert.org.cn

电话: 010-82990999